REMARKS

Claims 55-74 are pending in the application.

Claims 55-74 have been rejected.

Claims 55, 65, and 70 have been amended.

Claims 56 and 63 have been cancelled.

Rejection of Claims under 35 U.S.C. § 103(a)

Claims 55-60, 62, 63, 65-68 and 70-73 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,823,462 issued to Cheng et al. ("Cheng") in view of U.S. Patent 6,023,765 issued to Kuhn et al. ("Kuhn"). To the extent that they might be applied against the amended claims, Applicant respectfully traverses each of these rejections. Applicant respectfully submits that the arguments presented below with respect to independent claim 55 are generally applicable to claims 55-60, 62, 63, 65-68, and 70-73, as independent claims 65 and 70 generally require the same disputed limitations of claim 55, and claims 56-60, 62, 63, 66-68, and 71-73 depend from respective independent claims. Exemplary claim 55 recites:

> A method comprising:
> populating an access control list with a destination user group identifier, wherein
> said access control list is a role-based access control list,
> said destination user group identifier identifies a destination user group of a destination,
> said access control list comprises a source user group field configured to store a source user group identifier and a destination user group field configured to store a destination user group identifier,
> said source user group comprises a plurality of source network devices,
> said source user group is assigned to said source based on a role of said source,
> said destination user group comprises a plurality of destination network devices,
> said destination user group is assigned to said destination based on a role of said destination, and
> said access control list is configured to allow said source user group identifier and said destination user group identifier to be compared.

The Office Action cites Cheng as purportedly teaching the claimed access control list. Office Action, p.3 ("the group/category rules-based database is qualified as an access

control list"). Without conceding the point, Applicant respectfully submits that the rules database disclosed by the following section of Cheng is not even remotely comparable to the role-based access control list recited in amended claim 1.

> An example of an embodiment of a rules database is provided in FIG. 5 . In FIG. 5 , rules database 520 comprises a remote ID, e.g., group name, remote ID type, e.g., group name ID type, and At a security policy pointer which points to the particular security policy defined in the policy database. The remote ID and remote ID type refers to the ID and ID type of the nodes on the opposite end of the tunnels, e.g., client nodes, associated with a group name as a group.

Cheng 5:31-38 (cited at the Office Action, p. 3). Neither the cited passage, nor the remainder of Cheng discloses anything even comparable to the claimed access control list, as recited in claim 55. The claimed access control list contains a destination user group identifier (DUG) and a source user group (SUG) identifier, among other distinctions. Cheng's rules database is in no way comparable to the claimed access control list. For example, Cheng's rules database does not disclose a source user group identifier. *See* Cheng, FIG. 5 (element 520).

The Office Action cites another portion of Cheng as purportedly teaching a source user group:

> In FIG. 5 , tunnel definition database 530 in server node 110 A comprises the local ID, the local ID type, the remote ID and the remote ID type. The local ID and local ID type refers to the ID and ID type, e.g., IKE defined ID types such as Internet Protocol addresses, User@FQDN, FQDN, and X.500 Distinguished Name, of the server node 110 A.

Cheng 6:2-6 (cited at the Office Action, p. 3). Applicant notes that the cited portion discloses an entirely different database (a tunnel definition database) than the database the Office Action previously equated with the claimed access control list (a rules database). Applicant respectfully submist that the disclosed tunnel definition database is also not comparable to the claimed role-based access control list. Certainly the claimed access control list does not (and cannot) read on both Cheng's rules database and Cheng's tunnel definition database.

One of ordinary skill in the art would be expected to understand that access control lists are used to determine whether packets from a given source are allowed to pass to a given destination. The tunnel definition database disclosed by the cited passage of Cheng is incapable of providing any such functionality. This is unsurprising since Cheng is not directed towards access control lists, much less role-based access control lists. Instead, Cheng is directed towards configuring a plurality of different databases to establish a server node in a VPN with a single security policy for a group of tunnels. *See* Cheng, Abstract.

Even if one or more of the databases disclosed in the cited portions of Cheng were comparable to an access control list (a point which Applicant does not concede), certainly no successful comparison can be made between such database(s) and a role-based access control list. A role-based access control list, as claimed, includes a SUG assigned to a source based on a role of the source and a DUG assigned to a destination based on a role of the destination. To the contrary, Cheng discloses only the grouping of tunnels. And the grouping of tunnels is not based on a role of a source or destination, or any concept remotely related thereto. In fact, the word "role" does not appear even once in Cheng's specification. Instead, the grouping of tunnels disclosed in the cited portions of Cheng is based on having a single security policy for each tunnel associated with the group name. *See* Cheng 2:6-7.

Applicant further submits that neither Cheng nor Kuhn discloses that a "destination user group is assigned to said destination based on a role of said destination," as recited in amended claim 55. It is clear, based on the foregoing arguments, that Cheng does not group based on a role of group members. Nor do the cited portions of Kuhn disclose assigning a DUG based on a role of a destination. Role-based access is described by Kuhn as:

> Briefly stated, in role-based access control (RBAC) systems, access to an object within a computer system is provided to the members of groups termed "roles"; all subjects belonging to a given role have the same privileges to access various objects within the system. Individuals are then granted access to objects by being assigned membership in appropriate roles.

Kuhn 2:27-34 (cited at the Office Action, p. 3). As can be seen, there is no mention of a DUG, nor of assigning a DUG based on the role of a destination. This is unsurprising since the cited portions of Kuhn do not disclose populating role-based access control lists with a DUG identifier. Instead, Kuhn discloses using role based access control within a multi-level secure (MLS) system to grant users access to objects. Kuhn 3:40-41. Objects are defined by Kuhn as "documents, programs, facilities...within [a] computer system". Kuhn 1:25-26. So, Kuhn is directed toward restricting access to files or programs within a computer system. Kuhn is not directed toward populating a role-based access control list which controls access between source user groups and destination user groups.

Accordingly, Applicant respectfully requests the Examiner's reconsideration and withdrawal of the rejections to these claims and an indication of the allowability of same.

Claims 61, 64, 69 and 74 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cheng in view of Kuhn and in view of U. S. Patent 6,711,172 issued to Li ("Li"). Applicant respectfully traverses this rejection. The arguments and amendments above apply with equal force to these rejections. Accordingly, Applicant respectfully requests the Examiner's reconsideration and withdrawal of the rejections to these claims and an indication of the allowability of same.

CONCLUSION

In view of the amendments and remarks set forth herein, the application and the claims therein are believed to be in condition for allowance without any further examination and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is invited to telephone the undersigned at 512-439-5092.

If any extensions of time under 37 C.F.R. § 1.136(a) are required in order for this submission to be considered timely, Applicant hereby petitions for such extensions. Applicant also hereby authorizes that any fees due for such extensions or any other fee associated with this submission, as specified in 37 C.F.R. § 1.16 or § 1.17, be charged to deposit account 502306.

Respectfully submitted,

Shawn Doman
Attorney for Applicants
Reg. No. 60,362
Telephone: (512) 439-5092
Facsimile: (512) 439-5099